APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/107,618	06/30/1998	STEVEN M BLUMENAU	EMS-300US	8313

52427   7590   01/12/2010
MUIRHEAD AND SATURNELLI, LLC
200 FRIBERG PARKWAY, SUITE 1001
WESTBOROUGH, MA 01581

EXAMINER
STRANGE, AARON N

ART UNIT	PAPER NUMBER
2448	

MAIL DATE	DELIVERY MODE
01/12/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE
_____

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES
_____

Ex parte STEVEN M. BLUMENAU,
EREZ OFER, JOHN T. FITZGERALD,
JAMES M. McGILLIS, MARK C. LIPPITT,
and NATAN VISHLITZSKY
_____

Appeal 2009-002469
Application 09/107,618[1]
Technology Center 2400
_____

Decided: January 12, 2010
_____

Before LEE E. BARRETT, LANCE LEONARD BARRY, and
ST. JOHN COURTENAY III, *Administrative Patent Judges*.

BARRETT, *Administrative Patent Judge*.

DECISION ON APPEAL

This is a decision on appeal under 35 U.S.C. § 134(a) from the final

rejection of claims 1-4, 6-27, and 29-34. Claims 5 and 28 have been

canceled. We have jurisdiction pursuant to 35 U.S.C. § 6(b).

_____

    [1] Filed June 30, 1998, titled "Method and Apparatus for Providing
Data Management for a Storage System Coupled to a Network." The real
party in interest is EMC Corporation.

We reverse but enter new grounds of rejection as to claims 1
and 15-21.

<div align="center">STATEMENT OF THE CASE</div>

The invention

The invention relates to managing access to data at a shared storage
system, such a shared resource apportioned into volumes. One problem with
coupling multiple hosts to a shared storage system is that each host may be
able to access information that is proprietary to the other host processors.
Spec. 1, ll. 24-27. The invention provides three security techniques for
managing data: filtering, authentication, and validation. Spec. 2, ll. 7-12.

Filtering forwards only those requests for volumes that the device has
privileges to access. Spec. 4, ll. 1-3.

Because filtering is performed in response to the identity of the device
initiating the request, data security may be compromised if a device falsely
represents its identity to gain access to the resource. Authentication may be
used to verify that the device that is represented as the device issuing the
request is truly the device that issued the request. Spec. 4, ll. 8-17.

Validation may be provided to ensure that information, transferred
between the device and the shared resource is not corrupted (either
inadvertently or intentionally) during transit. Spec. 4, ll. 17-19.

Illustrative claim

Claim 1 is reproduced below for illustration:

1.   A data management method for managing access to a plurality of volumes of a storage system by at least two devices coupled to the storage system through a network, the method comprising steps of:

receiving over the network at the storage system a request from one of the at least two devices for access to at least one of the plurality of volumes of the storage system, the request identifying the at least one of the plurality of volumes in the storage system and a represented source of the request; and

selectively servicing the request, at the storage system, based at least in part on steps of:

determining, from configuration data, whether the represented source is authorized to access the at least one of the plurality of volumes; and

verifying that the represented source of the request is the one of the at least two devices that issued the request.

The references

The Examiner relies upon the following patents:

Yu	4,919,545	Apr. 24, 1990
Abadi	5,315,657	May 24, 1994
Boggs	5,959,994	Sept. 28, 1999
		(filed Aug. 19, 1996)
Ericson	6,061,753	May 9, 2000

Appellants cite numerous references describing the Small Computer System Interface (SCSI) protocol, including:

"SCSI FAQs," http://scsifaq.paralan.com/ (Mar. 19, 2007), 2 pages.
"SCSI FAQ Answers," http://scsifaq.paralan.com/scsifaqanswers.html (Mar. 19, 2007), 6 pages.
"How SCSI Works," http://computer.howstuffworks.com/scsi3.htm (Mar. 19, 2007), 2 pages.
"SCSI Connectors and SCSI Cable information," http://www.ramelectronics.net/html/scsi_connecters.html (Mar. 19, 2007), 4 pages.
"SCSI ID numbers," http://support.gateway.com/s/CDROM/ Panasonic/CS006aa/PANAS 100.shtml (Mar. 19, 2007), 1 page.
"SCSI-Initiator ID," http://www.sun.com/solutions/blueprints/ 0800/scsi.pdf (last visited Jan. 7, 2010).
"SCSI Table of Contents," http://www.ba-stuttgart.de/~schulte/htme/ ebuss12.htm#REF2.1.2 (last visited Jan. 7, 2010).

The rejections

Claims 1-4, 9-27, and 29-32 stand rejected under 35 U.S.C. § 103(a) as unpatentable over Ericson, Boggs, and Yu.

Claims 6-8, 33, and 34 stand rejected under 35 U.S.C. § 103(a) as unpatentable over Ericson, Boggs, and Yu, further in view of Abadi.

FINDINGS OF FACT

Ericson

Ericson is directed to controlling access to a target device 102 (e.g., a disk array) by initiators 100 interconnected by a Small Computer System Interface (SCSI) bus 104. The initiators 100 request access to the target 102 by directing an access message to the target 102 via the SCSI bus 104, the

message including the initiator identifier, a target identifier and a logical unit number (LUN) identifying the portion of the target device 102 to be accessed (i.e., the logical unit 108). Col. 3, lines 56- 63.

An initiator 100 may access only selected logical units 108 within the target 102. Col. 4, ll. 17-19. Access to the target device is controlled by a look-up structure preconfigured by a system operator who assigns selected logical units 108 in the target 102 to each of the initiators 100. When an initiator requests access, the look-up structure is indexed to check whether the initiator has been authorized to access the logical unit identified in the access message before allowing the initiator to access the logical unit. Col. 4, lines 26-65.

Yu

Yu describes that security techniques for protection of information in conventional computer and distributed system include capability based protection and access control list based protection. Col. 1, ll. 60-63.

Yu describes that objects can be identified and protected using a mechanism called "capability." A capability is a unique identifier of an object and a permission that gives a process the right to access the object. Col. 5, ll. 45-48. A conventional capability is a data structure that contains a unique object identifier (UID) and an access right (AR) to that object, where the access right field contains a mapping of bits of allowed interface operations. Col. 5, ll. 48-55. The possession of a capability for an object is sufficient for a process to access than object, if the interface operation is

legitimate. Col. 6, ll. 2-5. When a process requires access to objects at other network nodes, the capabilities for those objects must be transmitted to the network node where the object resides. Col. 6, ll. 37-40. However, "capabilities when transmitted from a network node become unprotected and can easily be forged, stolen, or modified." Col. 6, ll. 40-42.

Yu describes an authentication technique which uses encryption to provide a unique signature along with the capability. When that process wishes to access an object at a network node, the process transmits the capability, the signature, to a basic service element (a program) in the object, which then authenticates the capability and if the access is authorized, executes the basic service element and returns the result to the process. Col. 7, ll. 24-45. Thus, although an intruder can forge a capability by changing the object identifier and access rights fields, it cannot forge the signature. Col. 8, ll. 22-59.

CONTENTIONS

The Examiner finds that Ericson teaches a data management method for managing access to a plurality of volumes of a storage system by at least two devices coupled to the storage system through a network, which includes receiving a request for access to one of the volumes, the request identifying at least one of the volumes and a represented source of the request. The Examiner finds that Ericson does not teach verifying that the represented source of the request is one of the two devices, but that Yu teaches a security method for verifying the source. The Examiner concludes

that one of ordinary skill in the art would have been motivated to use both the access control of Ericson together with the authentication control of Yu to form an enhanced security system. Final Office Action 4-5.

The Examiner finds that Ericson teaches that his invention is applicable to Fibre Channel protocols and that Boggs teaches that the SCSI protocol may use Fibre Channel. The Examiner concludes that it would have been obvious to combine Boggs and Ericson to enable distributed access control over a wide area network. Final Office Action 4.

Appellants argue that Ericson describes a networked data storage system in a trusted environment where devices are trusted not to spoof (or are incapable of spoofing). Authentication is unnecessary in a trusted environment. By contrast, it is argued that Yu describes a network for providing services in an untrusted environment. Br. 10.[2]

Appellants argue that the Examiner has failed to provide the necessary motivation for the combination and has failed to present a prima facie case of obviousness. Br. 11. It is argued, with supporting evidence, that the SCSI interface in Ericson is local and secure and therefore trusted and secure. Accordingly, it is argued that it is unnecessary and undesirable to implement verification or authentication methods as disclosed by Yu in a SCSI environment as taught by Ericson. Br. 17-21.

Appellants argue that Boggs does not provide motivation to use Yu's authentication techniques in Ericson. It is argued that Ericson and Boggs disclose nothing about security issues present in untrusted environments, nor

_____

[2] References are to the Appeal Brief filed October 29, 2007.

describe Fibre Channel in the context of untrusted network environments.
Br. 13. It is argued that the fact that the Fibre Channel standard can be
adapted to support the SCSI protocol provides nothing at all suggesting that
the trusted environment of Ericson is somehow untrusted. *Id.* at 14. It is
argued that there is nothing intrinsically untrusted about the Fibre Channel
protocol, so Boggs provides no basis for the allegation that Ericson
contemplates an untrusted network environment. *Id.* at 15.

The Examiner responds that Ericson does mention the words "trust" or
"trusted environment." Ans. 9. It is stated that even if Appellants are
correct that the SCSI environment is a trusted environment, Ericson
discloses that the invention may be implemented using Fibre Channel
protocol which Appellants admit does not have the same inherent security.
It is further stated that Boggs teaches advantages of Fibre Channel and thus
it would have been obvious to use Fibre Channel in Ericson. *Id.* at 10. The
Examiner states that Appellants' entire argument rests on the inherent
security of a SCSI environment, but the rejection relies on the Fibre Channel
and that there is motivation to prevent identity spoofing on a distributed
Fibre Channel network using the technique of Yu. *Id.* at 11.

Appellants discuss at length the Examiner's assertions. Reply Br. 1-9.
In particular, it is noted that it is the Examiner's burden to show that Ericson
is not a trusted environment and would benefit from the authentication
technique of Yu, *id.* at 1-2; the Examiner has failed to consider the teachings
of Ericson as a whole, *id.* at 6-7; and that the Examiner has created the Fibre

Channel embodiment under a misguided sense that it supports an assertion that Ericson would benefit from the authentication technique of Yu, *id.* at 7.

ISSUE

Have Appellants shown that the Examiner has failed to establish a prima facie case of obviousness as to representative claim 1?

PRINCIPLES OF LAW

"[T]he best defense against the subtle but powerful attraction of a hindsight-based obviousness analysis is rigorous application of the requirement for a showing of the teaching or motivation to combine prior art references." *In re Dembiczak*, 175 F.3d 994, 999 (Fed. Cir. 1999). The motivation, suggestion or teaching may come explicitly from statements in the prior art, the knowledge of one of ordinary skill in the art, or, in some cases the nature of the problem to be solved. *Id.* In analyzing whether it would have been obvious to one of ordinary skill in the art to make a modification or combination, there does not have to be an express teaching, suggestion, or motivation (TSM) in a published article or issued patent. *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 419 (2007) ("The obviousness analysis cannot be confined by a formalistic conception of the words teaching, suggestion, and motivation, or by overemphasis on the importance of published articles and the explicit content of issued patents."). "To facilitate review [of the obviousness conclusion], this analysis should be made explicit." *Id.* at 418 (citing *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)).

ANALYSIS

The data management method of claim 1, and the storage system of claim 21 are commensurate in scope with each other and claim 1 will be considered as representative. The computer readable medium of claim 15 is directed to a data structure to be used in a method such as claim 1. Although claim 15 is different in scope than claims 1 and 21, it requires at least one identifier and also authentication information, and there is apparently no disagreement that claim 15 would have been obvious if claims 1 and 21 would have been obvious. Therefore, claim 15 stands or falls with claim 1.

The Board's job is to resolve disputed issues of fact and law. Although the teaching, suggestion, or motivation does not need to be expressly found in a reference, the Examiner must still provide convincing reasons for combining the teachings of the references.

In this case, we are persuaded by Appellants' arguments and supporting evidence that SCSI is a trusted environment and that Ericson describes only authorization in the context of a trusted environment. Although Ericson mentions that other protocols may be used, including the Fibre Channel protocol (col. 6, ll. 1-6), Ericson does not suggest that this would change the fundamental nature of the environment. We do not see that one skilled in the art would have been motivated to create a problem of an untrusted environment and then solve the problem with authentication.

The Examiner's motivation may be implicitly relying on the description of the Fibre Channel protocol in the Specification (page 1,

lines 19-27) as having the problems solved by the invention and then finding
that because Ericson could use a Fibre Channel protocol, it would
necessarily have the same problems. However, the Examiner has not shown
that Ericson is not a trusted environment or that implementing Ericson using
a Fibre Channel protocol necessarily produces an untrusted environment.
The Examiner appears to have created the rejection by finding a Fibre
Channel protocol and working backward using the description in the
Specification to create a problem to be solved. Because we find that Ericson
describes only a trusted environment, we find no motivation to add the
authentication procedure taught by Yu and conclude that the Appellants
have shown error in the Examiner's conclusion of obviousness as to claim 1.

The Examiner could have, but chose not to rely on Appellants'
admission of prior art at page 1 of the Specification for the use of
authorization in an untrusted environment. The Examiner might also have
found that Yu teaches authorization and authentication in an untrusted
environment and concluded that it would have been obvious to provide
access to volumes of a storage system instead of to generic objects in Yu in
view of the teachings in Ericson. These different reasons are set out in the
new ground of rejection *infra*.

CONCLUSION

Appellants have shown that the Examiner has failed to establish a
prima facie case of obviousness as to representative claim 1. The rejection
of claims 1-4, 9-27, and 29-32 is reversed. The reference to Abadi has not

been applied for the teachings missing in Ericson, Boggs, and Yu.
Accordingly, the rejection of claims 6-8, 33, and 34 is also reversed.

NEW GROUNDS OF REJECTION

1.

Claims 1, 15, and 21 are rejected under 35 U.S.C. § 103(a) as
unpatentable over Appellants' admitted prior art (APA) at Specification 1,
lines 19-33, Yu, and Ericson. Although we are reluctant to enter new
grounds of rejection at this late date, we feel that it is necessary in this case
to get Appellants' arguments on record.

Appellants describe that multiple hosts can be coupled over a network
to a shared data storage system. A problem with this arrangement is that
hosts may be physically able to access information belonging to other host
processors. One technique to solve the problem is to dedicate portions or
zones of memory to one or more of the hosts. We find that this teaches
"determining, from configuration data, whether the represented source is
authorized to access the at least one of the plurality of volumes" as recited in
claim 1. The Specification describes that this approach is still vulnerable to
individual actions of each host. Spec. 1, ll. 19-33. We assume this is a
description of admitted prior art (APA).

The teachings of Yu and Ericson have been previously described. Yu
teaches "determining, from configuration data, whether the represented
source is authorized to access [an object]" and "verifying that the
represented source of the request is the one of the at least two devices that

issued the request," as recited in claim 1 where the Yu's request is for access to a generic object rather than specifically to volumes of a storage system. Thus, Yu teaches authorization and authentication in a network environment. Furthermore, one of ordinary skill in the art would have recognized that the objects in Yu could be volumes of data storage devices as in Ericson.

One of ordinary skill in the art would have been motivated to provide authentication in addition to the authorization in the APA in view of Yu to prevent the prior art problem of spoofing since Yu recognized the problem and the solution. *See KSR*, 550 U.S. at 419-20 ("One of the ways in which a patent's subject matter can be proved obvious is by noting that there existed at the time of the invention a known problem for which there was an obvious solution encompassed by the patent's claims."); *Kahn*, 441 F.3d at 988 ("[T]he 'motivation-suggestion-teaching' test asks not merely what the references disclose, but whether a person of ordinary skill in the art, possessed with the understandings and knowledge reflected in the prior art, and motivated by the general problem facing the inventor, would have been led to make the combination recited in the claims.").

Alternatively, one of ordinary skill in the art would have recognized that the generic objects in Yu could be volumes of a storage system in view of Ericson. One of ordinary skill in the art would have been motivated to use stored lookup tables as recited in claim 15 to store authorization and authentication information in view of Yu and Ericson. We leave it to the Examiner to consider the patentability of the dependent claims.

2.

Claims 15-20 stand rejected under 35 U.S.C. § 103(a) as unpatentable over Yu. Claims 15-20 recite a data structure on a computer readable medium. Descriptive material is not entitled to patentable weight unless there is a functional relationship to the substrate. *In re Gulack*, 703 F.2d 1381, 1386 (Fed. Cir. 1983); *Ex parte Nehls*, 88 USPQ2d 1883, 1887-90 (BPAI 2008); *Ex parte Curry*, 84 USPQ2d 1272 (BPAI 2005) (nonprecedential) (Fed. Cir. Appeal No. 2006-1003, *aff'd* Fed. Cir. R. 36 June 12, 2006). Here, a data structure is only an arrangement of data that bears no functional relationship to the substrate (computer readable medium) that stores the data and it is not entitled to patentable weight. The lack of functional relationship is evidenced by the generic nature of the claimed "computer readable medium," which could be any structure. Limitations of how the storage system will use the data structure are considered to be statements of intended use which are not entitled to patentable weight.

CONCLUSION

The rejections of claims 1-4, 6-27, and 29-34 are reversed.

New grounds of rejection are entered as to claims 1 and 15-21.

This decision contains new grounds of rejection pursuant to 37 C.F.R. § 41.50(b). 37 C.F.R. § 41.50(b) provides that "[a] new ground of rejection pursuant to this paragraph shall not be considered final for judicial review."

37 C.F.R. § 41.50(b) also provides that the appellant, WITHIN TWO MONTHS FROM THE DATE OF THE DECISION, must exercise one of

the following two options with respect to the new ground of rejection to

avoid termination of the appeal as to the rejected claims:

      (1) *Reopen prosecution*. Submit an appropriate amendment of
the claims so rejected or new evidence relating to the claims so
rejected, or both, and have the matter reconsidered by the examiner, in
which event the proceeding will be remanded to the examiner. . . .

      (2) *Request rehearing*. Request that the proceeding be reheard
under § 41.52 by the Board upon the same record. . . .

Requests for extensions of time are governed by 37 C.F.R. § 1.136(b).
See 37 C.F.R. § 41.50(f).

<div align="center">REVERSED -- 37 C.F.R. § 41.50(b)</div>

erc

MUIRHEAD AND SATURNELLI, LLC
200 FRIBERG PARKWAY, SUITE 1001
WESTBOROUGH MA 01581